REMARKS

Claims 1-49 are pending in this application.

Claims 1, 14, 26, 39, and 43 are independent.

The Examiner's notice that claims 8-10, 20-24, 31-34, and 43-49 would be allowable if rewritten in independent form to include all of the limitations of the respective base claims and any intervening claims is noted with appreciation. However, the Examiner's attention is courteously directed to claim 43, which is an independent claim. The Examiner's objection to independent claim 43 is not understood. As acknowledged by the Examiner, the limitations of independent claim 43 are not disclosed in the prior art, thus an amendment of independent claim 43 is not necessary, nor required, to make it allowable. Accordingly, it is respectfully requested that the Examiner withdraw the objection to independent claim 43, as well as that to claims 44-49 which depend from independent claim 43, and indicate claims 43-49 as allowable.

Claims 1, 7, 12-14, 25-26, 35, and 37-38 stand rejected under 35 U.S.C. §102(e) as anticipated by Powar (U.S. Patent No. 6,285,991). The rejection is respectfully traversed.

Independent claim 1 is directed to a networked system for accessing information. This claim requires, at least in part, encryption of a first component message with a first crypt-key by a first network station; encryption of a second component message with a second crypto-key by a second network station; a combining of the first encrypted message and the second encrypted message and a transmission of the combined message by the second network station; a receipt of the transmitted combined message and retransmission of the received combined message by a third network station; and a receipt of the retransmitted combined message by the first network station.

The first network station, which is associated with a first network entity, controls access to information stored on a network for a third network entity associated with the third network station. The second network station, which is associated with a second network entity, controls access to the network by the third network entity. After the retransmitted combined message is received at the first network station from the third network station, which is associated with the third network entity, the first network station decrypts the two encrypted component

messages (included in the retransmitted combined message) and controls access to the stored information based on the two decrypted component messages.

Regarding independent claim 1, the Examiner argues that the Powar reference teaches the required limitations. In particular, the Examiner argues that the biller of Figure 1 corresponds to the first network station controlling access to information stored on a network for a third network entity; that the certified bank, disclosed at column 6, lines 63-64, corresponds to the second network station controlling access to the network by the third network entity; and that the customer of Figure 1 corresponds to the third network station further transmitting a combined encrypted component message.

The Examiner further points to the disclosure of column 9, lines 1-8, which discusses the certified bank issuing a certificate to the customer. As best understood, the Examiner's position is that this customer certificate corresponds to the second component message. Also, the Examiner points to column 9, lines 49-52, and argues that the customer combines the certificate with a request to activate electronic biller and further transmits the combination to the biller to obtain access to stored information. According to the Examiner, and with reference to column 10, lines 28-61, after the biller receives the further transmission from the customer, the biller performs operations to begin an electronic billing service to the customer.

It is respectfully noted that the Examiner's rejection of independent claim 1 is not understood. Not only has the Examiner failed to address certain limitations of the claim in the rejection, but also the Examiner has misread and misapplied the Powar reference.

Discussed above, claim 1 requires that the first network station encrypt a first component message with a first crypto-key associated with the first network entity. The Examiner has completely ignored this limitation. In other words, nowhere in the rejection is it argued that the biller (which the Examiner contends corresponds to the first network station) encrypts a first component message with a first crypto-key, nor is this requirement otherwise addressed.

Yet another limitation of claim 1 that has not been addressed by the Examiner is the requirement that the second network station (the certified bank, according to the Examiner) encrypt a second component message. Nowhere does the Examiner argue that a second network station (the certified bank, according to the Examiner)

perform such an encryption, nor is the required encryption by the second network station otherwise addressed.

Also as discussed above, claim 1 requires that the second network station combine the encrypted first component message with a second encrypted component message. This limitation too seems to have been ignored. While the Examiner does argue, albeit incorrectly, that the customer combines messages, the customer, according to the Examiner's arguments, corresponds to the third network station, not the second network station.

Still another limitation of claim 1 that has not been addressed in the rejection is the requirement that the third network station receive a transmitted combined component message. This limitation simply isn't addressed in the rejection.

Yet another requirement of claim 1 that has not been addressed is the recited decryption of the first and second encrypted component messages included in the received further transmitted combined messages at the first network station. At best, the Examiner referenced text shows decryption of a digital signature.

Thus, the Examiner has not considered at least the above-mentioned requirements in rejecting claim 1, and thus the rejection is improper.

In addition to not addressing certain limitations, the rejection also fails to apply Powar for what it teaches. In particular, the referenced portions of Powar teach a customer obtaining a certificate from a certified bank (column 6, lines 63-64, and column 9, lines 1-42). When the customer obtains a certificate, he obtains a public/private key pair. Powar does not teach or suggest that delivery of the certificate from the certified bank to the customer is an encrypted delivery. Rather, Powar teaches, in one alternative, that a private key is delivered to the customer.

After the customer obtains a certificate, the customer makes a request to the biller to begin to receive electronic bills (column 10, lines 15-27). More particularly, the customer sends a request message via email to the biller via a network. The request message includes the request for electronic billing service, and a copy of the customer's certificate. The request message is digitally signed by the customer. The customer's digital signature is simply a message digest of the request for service encrypted with the private key of the customer. Thus, only one portion of the request message is encrypted.

Once the biller receives the request message, the biller authenticates the request (column 10, lines 28-40). Authentication of the message includes the biller

authenticating the received customer certificate. If the certificate is authenticated, the biller receives a copy of the customer's public key. This public key is then used to decrypt the digital signature. Decryption of the signature reveals the message digest produced by the customer. The biller then compares the decrypted message digest with a message digest of the unencrypted service request included in the request message. If the two are the same, the customer is authenticated.

Thus, at most, Powar teaches a customer obtaining a certificate (and associated public/private key pair). The customer then simply uses the private key to sign a request to begin to receive electronic bills, not to access stored information. The customer emails the request to the biller, the biller obtains the customer's public key and authenticates the customers. As should be clear from the discussion of the requirements of claim 1 above, Powar in no way teaches or suggests the invention recited in claim 1.

Accordingly, in view of the above, it is respectfully requested that the Examiner reconsider and withdraw the rejection of claim 1, as well as claims 2-7 and 11-13 which depend from independent claim 1.

Additionally, it seems that the Examiner has failed to consider limitations recited in dependent claims 12 and 13. As an example, the Examiner does not point out where in Powar the requirement of claim 12 that the first network station be further configured to combine the encrypted first component message with a network address for the stored information is taught. None of the other requirements of claim 12, and none of the requirements of claim 13 are addressed in the rejection. Accordingly, for this reason alone, it is respectfully requested that the Examiner reconsider and withdraw the rejection of dependent claims 12 and 13.

As to the rejection of independent claims 14 and 26, the Examiner, as best can be understood, relies upon the arguments made in rejecting independent claim 1 in rejecting independent claims 14 and 26. However, both independent claim 14 and independent claim 26 include limitations not included in independent claim 1. Thus, the Examiner has not considered limitations in each of independent claims 14 and 26, and the rejection is improper.

Accordingly, it is respectfully requested that the Examiner reconsider and withdraw the rejection of independent claims 14 and 26, as well as dependent claims 15-19 and 25, which depend from claim 14, and dependent claims 27-30, and 35-38, which depend from claim 26.

Claims 2-6, 15-19, 27-30, and 39-41 stand rejected under 37 U.S.C. §103(a) as obvious over, Powar in view of Fox (U.S. Patent No. 6,560,581). The rejection is respectfully traversed.

Regarding independent claim 39, the rejection is not understood. First, the Examiner does not specifically address any limitations of the claim. Thus, for this reason alone, the rejection is improper. Further, as best understood, the Examiner does not rely upon Fox in rejecting claim 39. Rather, the Examiner seems to rely exclusively upon Powar. Thus, why claim 39 and its dependencies are rejected as being obvious is not clear. Accordingly, it is respectfully requested that the Examiner reconsider and withdraw the rejection of claim 39, as well as the rejection of claims 40 and 41 which depend from claim 39.

Regarding dependent claims 2-6, 15-19, and 27-30, and 40-41 the Examiner acknowledges that Powar does not disclose various features associated with crypto-keys, including, but not limited to, a first crypto-key being symmetric, and a second crypto-key being non-symmetric; and a symmetric crypto key known only to the first network entity. The Examiner looks to Fox for various limitations related to crypto-keys recited in claims 2-6, 15-19, 27-30, and 40-41.

While Fox may disclose crypto-keys used in electronic commerce, a combination of Fox with Powar would certainly not make obvious any of the rejected claims. As should be understood from the discussion above, Powar does not teach or suggest the independent claims from which claims 2-6, 15-19, and 27-30, and 40-41 depend. A combination of Fox with Powar does not cure this deficiency. Additionally, how one would combine Powar and Fox, and what the result would be is entirely speculative. The Examiner has provided no guidance as to how such a combination could be achieved, nor has proper motivation for such a combination been provided.

Thus, for at least these reasons, it is respectfully requested that the Examiner reconsider and withdraw the rejection of dependent claims 2-6, 15-19, and 27-30, and 40-41.

Claims 11 and36 stand rejected under 37 U.S.C. §103(a) as obvious over, Powar in view of Fox, and further in view of Sirbu (U.S. Patent No. 5,809,144). The rejection is respectfully traversed.

Claims 11 and 36 require a timestamp, which the Examiner acknowledges is not taught in Powar or Fox. The Examiner looks to Sirbu for such. While Sirbu does

teach a timestamped message, such a combination fails to cure the defects noted above. Namely, neither Power, or a combination of Powar and Fox teach any of the independent claims of the present application. Furthermore, the Examiner has again provided no guidance as to how the timestamp of Fox could be combined with Powar and Fox. Accordingly, for at least these reasons, it is respectfully requested that the Examiner reconsider and withdraw the rejection of claim 11 and 16.

The art cited by the Examiner but not relied upon in rejecting the claims has been reviewed and found not to disclose the invention as claimed in the present application.

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed local telephone number, in order to expedite resolution of any remaining issues and further to expedite passage of the application to issue, if any further comments, questions or suggestions arise in connection with the application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 01-2135 and please credit any excess fees to such deposit account.

Respectfully submitted,
ANTONELLI, TERRY, STOUT & KRAUS, LLP

Sterling W. Chandler
Registration No. 51,370
Telephone: 703-236-6081
schandler@antonelli.com

SWC